

AMENDED IN SENATE MAY 21, 2015

AMENDED IN SENATE APRIL 6, 2015

SENATE BILL

No. 570

Introduced by Senator Jackson

February 26, 2015

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 570, as amended, Jackson. Personal information: privacy: breach.

Existing law requires a person or business conducting business in California and any agency, as defined, that owns or licenses computerized data that includes personal information, as defined, to disclose a breach of the security of the system in the most expedient time possible and without unreasonable delay, as specified. Existing law requires a person, business, or agency that is required to issue a security breach notification to meet specific requirements, *including that the notification be written in plain language.*

This bill would additionally require ~~that the security breach notification include a one-page notice containing specified information.~~ *to be titled "Notice of Data Breach," to present the content under prescribed headings, and, in the case of written notices, to present the information on one page. The bill would prescribe a model security breach notification form.*

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language and shall include a one page notice language, shall be titled "Notice of Data Breach," in which the content is presented and shall present the content under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." *In the case of written notices, as specified in paragraph (1) of subdivision (i), the information shall be presented on one page.* Additional information may be provided as a supplement to the one page notice.

(A) The format of the one page notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the one page notice shall be clearly and conspicuously displayed.

(C) The text of the one page notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) *Use of the model security breach notification form prescribed below shall constitute compliance with this paragraph, although use of the model security breach notification form is not required.*

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		

1 2 3 4 5	<i>What You Can Do.</i>	
6 7 8 9 10 11 12 13 14	<i>Other Important Information.</i> <i>[insert other important information]</i>	
15 16 17 18 19	<i>For More Information.</i>	<i>Call [telephone number] or go to [Web site]</i>

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security

1 number or a driver's license or California identification card
2 number.

3 (3) At the discretion of the agency, the security breach
4 notification may also include any of the following:

5 (A) Information about what the agency has done to protect
6 individuals whose information has been breached.

7 (B) Advice on steps that the person whose information has been
8 breached may take to protect himself or herself.

9 ~~(4) In the case of a breach of the security of the system involving~~
10 ~~personal information defined in paragraph (2) of subdivision (g)~~
11 ~~for an online account, and no other personal information defined~~
12 ~~in paragraph (1) of subdivision (g), the agency may comply with~~
13 ~~this section by providing the security breach notification in~~
14 ~~electronic or other form that directs the person whose personal~~
15 ~~information has been breached to promptly change his or her~~
16 ~~password and security question or answer, as applicable, or to take~~
17 ~~other steps appropriate to protect the online account with the~~
18 ~~agency and all other online accounts for which the person uses the~~
19 ~~same user name or email address and password or security question~~
20 ~~or answer.~~

21 ~~(5) In the case of a breach of the security of the system involving~~
22 ~~personal information defined in paragraph (2) of subdivision (g)~~
23 ~~for login credentials of an email account furnished by the agency,~~
24 ~~the agency shall not comply with this section by providing the~~
25 ~~security breach notification to that email address, but may, instead,~~
26 ~~comply with this section by providing notice by another method~~
27 ~~described in subdivision (i) or by clear and conspicuous notice~~
28 ~~delivered to the resident online when the resident is connected to~~
29 ~~the online account from an Internet Protocol address or online~~
30 ~~location from which the agency knows the resident customarily~~
31 ~~accesses the account.~~

32 (e) Any agency that is required to issue a security breach
33 notification pursuant to this section to more than 500 California
34 residents as a result of a single breach of the security system shall
35 electronically submit a single sample copy of that security breach
36 notification, excluding any personally identifiable information, to
37 the Attorney General. A single sample copy of a security breach
38 notification shall not be deemed to be within subdivision (f) of
39 Section 6254 of the Government Code.

(f) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, “personal information” means either of the following:

(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver’s license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

(D) Medical information.

(E) Health insurance information.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(h) (1) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, “health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

(i) For purposes of this section, “notice” may be provided by one of the following methods:

1 (1) Written notice.

2 (2) Electronic notice, if the notice provided is consistent with
3 the provisions regarding electronic records and signatures set forth
4 in Section 7001 of Title 15 of the United States Code.

5 (3) Substitute notice, if the agency demonstrates that the cost
6 of providing notice would exceed two hundred fifty thousand
7 dollars (\$250,000), or that the affected class of subject persons to
8 be notified exceeds 500,000, or the agency does not have sufficient
9 contact information. Substitute notice shall consist of all of the
10 following:

11 (A) Email notice when the agency has an email address for the
12 subject persons.

13 (B) Conspicuous posting, for a minimum of 30 days, of the
14 notice on the agency's Internet Web site page, if the agency
15 maintains one. For purposes of this subparagraph, conspicuous
16 posting on the agency's Internet Web site means providing a link
17 to the notice on the home page that is in larger type than the
18 surrounding text, or in contrasting type, font, or color to the
19 surrounding text of the same size, or set off from the surrounding
20 text of the same size by symbols or other marks that call attention
21 to the link.

22 (C) Notification to major statewide media and the Office of
23 Information Security within the Department of Technology.

24 (4) *In the case of a breach of the security of the system involving*
25 *personal information defined in paragraph (2) of subdivision (g)*
26 *for an online account, and no other personal information defined*
27 *in paragraph (1) of subdivision (g), the agency may comply with*
28 *this section by providing the security breach notification in*
29 *electronic or other form that directs the person whose personal*
30 *information has been breached to promptly change his or her*
31 *password and security question or answer, as applicable, or to*
32 *take other steps appropriate to protect the online account with the*
33 *agency and all other online accounts for which the person uses*
34 *the same user name or email address and password or security*
35 *question or answer.*

36 (5) *In the case of a breach of the security of the system involving*
37 *personal information defined in paragraph (2) of subdivision (g)*
38 *for login credentials of an email account furnished by the agency,*
39 *the agency shall not comply with this section by providing the*
40 *security breach notification to that email address, but may, instead,*

1 *comply with this section by providing notice by another method*
2 *described in this subdivision or by clear and conspicuous notice*
3 *delivered to the resident online when the resident is connected to*
4 *the online account from an Internet Protocol address or online*
5 *location from which the agency knows the resident customarily*
6 *accesses the account.*

7 (j) Notwithstanding subdivision (i), an agency that maintains
8 its own notification procedures as part of an information security
9 policy for the treatment of personal information and is otherwise
10 consistent with the timing requirements of this part shall be deemed
11 to be in compliance with the notification requirements of this
12 section if it notifies subject persons in accordance with its policies
13 in the event of a breach of security of the system.

14 (k) Notwithstanding the exception specified in paragraph (4) of
15 subdivision (b) of Section 1798.3, for purposes of this section,
16 “agency” includes a local agency, as defined in subdivision (a) of
17 Section 6252 of the Government Code.

18 SEC. 2. Section 1798.82 of the Civil Code is amended to read:

19 1798.82. (a) A person or business that conducts business in
20 California, and that owns or licenses computerized data that
21 includes personal information, shall disclose a breach of the
22 security of the system following discovery or notification of the
23 breach in the security of the data to a resident of California whose
24 unencrypted personal information was, or is reasonably believed
25 to have been, acquired by an unauthorized person. The disclosure
26 shall be made in the most expedient time possible and without
27 unreasonable delay, consistent with the legitimate needs of law
28 enforcement, as provided in subdivision (c), or any measures
29 necessary to determine the scope of the breach and restore the
30 reasonable integrity of the data system.

31 (b) A person or business that maintains computerized data that
32 includes personal information that the person or business does not
33 own shall notify the owner or licensee of the information of the
34 breach of the security of the data immediately following discovery,
35 if the personal information was, or is reasonably believed to have
36 been, acquired by an unauthorized person.

37 (c) The notification required by this section may be delayed if
38 a law enforcement agency determines that the notification will
39 impede a criminal investigation. The notification required by this

section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language and shall include a one page notice *language, shall be* titled “Notice of Data Breach,” ~~in which the content is presented~~ *and shall present the content* under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” *In the case of written notices, as specified in paragraph (1) of subdivision (j), the information shall be presented on one page.* Additional information may be provided as a supplement to the one page notice.

(A) The format of the one page notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the one page notice shall be clearly and conspicuously displayed.

(C) The text of the one page notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) Use of the model security breach notification form prescribed below shall constitute compliance with this paragraph, although use of the model security breach notification form is not required.

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		

1 2 3 4 5 6	<i>What Information Was Involved?</i>	
7 8 9 10 11 12	<i>What We Are Doing.</i>	
13 14 15 16 17 18 19	<i>What You Can Do.</i>	
20 21 22 23 24 25 26 27 28	<i>Other Important Information.</i> <i>[insert other important information]</i>	
29 30 31 32 33	<i>For More Information.</i>	<i>Call [telephone number] or go to [Web site]</i>

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

1 (C) If the information is possible to determine at the time the
2 notice is provided, then any of the following: (i) the date of the
3 breach, (ii) the estimated date of the breach, or (iii) the date range
4 within which the breach occurred. The notification shall also
5 include the date of the notice.

6 (D) Whether notification was delayed as a result of a law
7 enforcement investigation, if that information is possible to
8 determine at the time the notice is provided.

9 (E) A general description of the breach incident, if that
10 information is possible to determine at the time the notice is
11 provided.

12 (F) The toll-free telephone numbers and addresses of the major
13 credit reporting agencies if the breach exposed a social security
14 number or a driver's license or California identification card
15 number.

16 (G) If the person or business providing the notification was the
17 source of the breach, an offer to provide appropriate identity theft
18 prevention and mitigation services shall be provided at no cost to
19 the affected person for not less than 12 months along with all
20 information necessary to take advantage of the offer to any person
21 whose information was or may have been breached if the breach
22 exposed or may have exposed personal information defined in
23 subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

24 (3) At the discretion of the person or business, the security
25 breach notification may also include any of the following:

26 (A) Information about what the person or business has done to
27 protect individuals whose information has been breached.

28 (B) Advice on steps that the person whose information has been
29 breached may take to protect himself or herself.

30 ~~(4) In the case of a breach of the security of the system involving~~
31 ~~personal information defined in paragraph (2) of subdivision (h)~~
32 ~~for an online account, and no other personal information defined~~
33 ~~in paragraph (1) of subdivision (h), the person or business may~~
34 ~~comply with this section by providing the security breach~~
35 ~~notification in electronic or other form that directs the person whose~~
36 ~~personal information has been breached promptly to change his~~
37 ~~or her password and security question or answer, as applicable, or~~
38 ~~to take other steps appropriate to protect the online account with~~
39 ~~the person or business and all other online accounts for which the~~
40 ~~person whose personal information has been breached uses the~~

1 same user name or email address and password or security question
2 or answer.

3 ~~(5) In the case of a breach of the security of the system involving~~
4 ~~personal information defined in paragraph (2) of subdivision (h)~~
5 ~~for login credentials of an email account furnished by the person~~
6 ~~or business, the person or business shall not comply with this~~
7 ~~section by providing the security breach notification to that email~~
8 ~~address, but may, instead, comply with this section by providing~~
9 ~~notice by another method described in subdivision (j) or by clear~~
10 ~~and conspicuous notice delivered to the resident online when the~~
11 ~~resident is connected to the online account from an Internet~~
12 ~~Protocol address or online location from which the person or~~
13 ~~business knows the resident customarily accesses the account.~~

14 (e) A covered entity under the federal Health Insurance
15 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d
16 et seq.) will be deemed to have complied with the notice
17 requirements in subdivision (d) if it has complied completely with
18 Section 13402(f) of the federal Health Information Technology
19 for Economic and Clinical Health Act (Public Law 111-5).
20 However, nothing in this subdivision shall be construed to exempt
21 a covered entity from any other provision of this section.

22 (f) A person or business that is required to issue a security breach
23 notification pursuant to this section to more than 500 California
24 residents as a result of a single breach of the security system shall
25 electronically submit a single sample copy of that security breach
26 notification, excluding any personally identifiable information, to
27 the Attorney General. A single sample copy of a security breach
28 notification shall not be deemed to be within subdivision (f) of
29 Section 6254 of the Government Code.

30 (g) For purposes of this section, “breach of the security of the
31 system” means unauthorized acquisition of computerized data that
32 compromises the security, confidentiality, or integrity of personal
33 information maintained by the person or business. Good faith
34 acquisition of personal information by an employee or agent of
35 the person or business for the purposes of the person or business
36 is not a breach of the security of the system, provided that the
37 personal information is not used or subject to further unauthorized
38 disclosure.

39 (h) For purposes of this section, “personal information” means
40 either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

1 (A) Email notice when the person or business has an email
2 address for the subject persons.

3 (B) Conspicuous posting, for a minimum of 30 days, of the
4 notice on the Internet Web site page of the person or business, if
5 the person or business maintains one. For purposes of this
6 subparagraph, conspicuous posting on the agency's Internet Web
7 site means providing a link to the notice on the home page that is
8 in larger type than the surrounding text, or in contrasting type,
9 font, or color to the surrounding text of the same size, or set off
10 from the surrounding text of the same size by symbols or other
11 marks that call attention to the link.

12 (C) Notification to major statewide media.

13 (4) *In the case of a breach of the security of the system involving*
14 *personal information defined in paragraph (2) of subdivision (h)*
15 *for an online account, and no other personal information defined*
16 *in paragraph (1) of subdivision (h), the person or business may*
17 *comply with this section by providing the security breach*
18 *notification in electronic or other form that directs the person*
19 *whose personal information has been breached promptly to change*
20 *his or her password and security question or answer, as applicable,*
21 *or to take other steps appropriate to protect the online account*
22 *with the person or business and all other online accounts for which*
23 *the person whose personal information has been breached uses*
24 *the same user name or email address and password or security*
25 *question or answer.*

26 (5) *In the case of a breach of the security of the system involving*
27 *personal information defined in paragraph (2) of subdivision (h)*
28 *for login credentials of an email account furnished by the person*
29 *or business, the person or business shall not comply with this*
30 *section by providing the security breach notification to that email*
31 *address, but may, instead, comply with this section by providing*
32 *notice by another method described in this subdivision or by clear*
33 *and conspicuous notice delivered to the resident online when the*
34 *resident is connected to the online account from an Internet*
35 *Protocol address or online location from which the person or*
36 *business knows the resident customarily accesses the account.*

37 (k) Notwithstanding subdivision (j), a person or business that
38 maintains its own notification procedures as part of an information
39 security policy for the treatment of personal information and is
40 otherwise consistent with the timing requirements of this part, shall

1 be deemed to be in compliance with the notification requirements
2 of this section if the person or business notifies subject persons in
3 accordance with its policies in the event of a breach of security of
4 the system.

O